REMARKS/ARGUMENTS

Claims 1-8 and 10-79 are pending. Claims 1, 5, 34 and 39 are amended and claim 9 is canceled.

Claims 1-79 are again rejected under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse** (US 6,005,945) in view of Pang (US 6,446,204). Applicant notes that the current Office action (mailed on March 13, 2007) is the **tenth Office action** received from the (same) Examiner, all of which cite **Whitehouse** as the primary reference. However, Applicant has repeatedly argued in detail that Whitehouse does not disclose a number of the limitations present in the independent and dependent claims. Applicant respectfully request that each and every one of the arguments articulated below, specially the ones regarding **Whitehouse** (including those with regard to dependent claims 5 and 6) be sufficiently addressed by the Examiner.

Claim 1 includes, among other limitations, "a stateless cryptographic module to authenticate any of the plurality of users using one or more of the plurality of security device transaction data records stored in the database, in a stateless manner." Applicant respectfully submits that the combination of Whitehouse and Pang, alone or in combination does not teach or suggest the above limitation.

This time, the Examiner admits that Whitehouse does not disclose or suggest the above limitation (and the limitation of "a scalable server system communicating with the client system over a communication network . . . , wherein the scalable server system is configured to process each security device transaction data record in a stateless manner"). (Office action, last sentence of page 2 through the first sentence on page 3.). However, the Examiner cites Abstract, FIGs. 2, 6, and 8, col. 23, lines 24-64, and col. 25, lines 1-20 of Pang as disclosing the above (unamended) limitation. Applicant respectfully disagrees for the following reasons.

First, Applicant fails to find any disclosure in Pang about the authentication engines 802, 804, and 806 being "stateless" and being able to "authenticate. . . in a stateless manner." Although Pang discloses that "In identifying a particular authentication engine [and host], the object request broker 282 uses a load balancing scheme to attempt to balance the work load of

the authentication engines [and hosts]" (col. 23, lines 42-45 and 55-58), one skilled in the art would readily understand that this "load balancing" is not the same as authenticating "in a stateless manner."

Pang defines load balancing as "the ability to distribute cartridge instance execution across multiple machines." (Col. 6, lines 35-38, underlining added.). Furthermore, Pang emphasizes that "resource manager 254 applies a set of load balancing rules to determine where to initiate instances of cartridges where there is more than one possible host machine." (Col. 10, lines 32-35, underlining added.).

In contrast, the specification defines "stateless" as "each cryptographic module is a stateless device, meaning that a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package." (Page 8, lines 16-19, underlining added.). Accordingly, one skilled in the art would readily understand that this determination of "where to initiate instances of cartridges where there is more than one possible host machine" is not the same as authenticating "in a stateless manner," wherein the application "does not rely upon any information about what occurred with the previous PSD package." As a result, the combination of Whitehouse/Pang, alone or in combination, does not teach or suggest (authenticating) "**in a stateless manner**."

Second, Pang does not teach or suggest a "cryptographic module to authenticate any of the plurality of users. . . , in a stateless manner."

The authentication engines 802, 804, and 806 of Pang do NOT perform the authentication function. Rather, it is the provider(s) that perform the authentication function. "Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser requests that are associated with a particular username and password pair Another example of a type of provider that may be associated with authentication host is an IP address provider. The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address.. (Col. 20, lines 26-47, underlining added.).

Pang is very clear about which modules/devices perform the authentication function (that is, the providers, as explained above). Pang emphasizes that "[o]nce the providers have completed the authentication of the provider requests, they send response messages back to the authentication engine . . .. Upon receiving the response messages from the one or more providers, the authentication engine performs any necessary logical operations on the returned response messages. The authentication engine then notifies the dispatcher whether the browser request should be forwarded to the appropriate cartridge or that the sending browser should be notified that access was denied." (Col. 23, line 65 to col. 7, line 6, underlining added.).

Therefore, it is clear from the above that the authentication modules (that is, the providers) of Pang are not capable of authenticating any of the plurality of users, because the Providers that are responsible for authentication each perform "a specific authentication function to restrict access to a particular cartridge." For example, BASIC Provider, IP Provider, DOMAIN name Provider, etc.. Furthermore, the authentication in Pang is NOT performed for "any of the users . . . in a stateless manner." As a result, the combination of Whitehouse/Pang, alone or in combination, does not teach or suggest "**authenticating any of the plurality of users**. . . **in a stateless manner**."

Fourth, Applicant still fails to see any **motivation to combine** Pang with Whitehouse. The Examiner states that it would have been obvious to one skilled in the art to modify Whitehouse's system to include Pang's stateless cryptographic modules "because this would have ensure [sic] that client would be properly authenticate [sic] whenever service is needed." Applicant respectfully disagrees.

First, as explained above, there is no stateless cryptographic modules in Pang. Second, it is not possible, without major architectural changes and a major overhaul of the system, as described above with respect to "first argument," to make the Whitehouse system a system with "load balancing" feature, as described by Pang. Third, even if one could make the Whitehouse system a "scalable" system the "scalable" client-server environment does not enhance the authentication process of the system of Whitehouse. In fact, by making the Whitehouse environment a "scalable environment" as defined by Pang, the system of Whitehouse becomes

enhanced with respect to the authentication function, because multiple providers would be needed and multiple copies of the cryptographic keys need to be generated and stored in the local memories of the Whitehouse's computers. Fourth, each of the Whitehouse and Pang references are **individually complete** and **functional in itself**, one skilled in the art of computer authentication would see no reason to add parts to any of them. For example, one skilled in the art of computer authentication would readily appreciate that adding the "scalable environment" of Pang will not enhance the authentication of Whitehouse system, because Whitehouse system is already using a central computer to authenticate its users.

In short, based on at least the above-mentioned **four arguments**, each of which deemed sufficient by itself, the independent claim 1 is patentable over cited references.

Independent claim 39 includes, among other limitations, "authenticating by a scalable cryptographic module any of the plurality of the users in a stateless manner." As discussed above, the combination of Whitehouse and Pang does not teach or suggest the above limitations. Consequently, claim 39 is also patentable over cited references.

Dependent claim 5 includes the additional limitation of "further comprising at least one more stateless cryptographic module, wherein each cryptographic module is configured to process any of the plurality of security device transaction data records," and **dependent claim 6** includes the additional limitation of "wherein a user can be authenticated using any of the cryptographic modules." Applicant respectfully disagree with the assertion that Whitehouse in column 9, lines 51-63 discloses the above two limitations. (See, Office action, page 4, paragraphs no. 8 and 9.). The cited text in Whitehouse teaches a process for generating a new session key and does not teach an additional cryptographic module that is "configured to process any of the plurality of security device transaction data records," or "wherein a user can be authenticated using any of the cryptographic modules."

In fact, as it has been argued again and again in the past several responses to the previous nine Office action, Whitehouse's central computers 102 cannot "process any of the plurality of security device transaction data records," because each central computer 102 of Whitehouse stores the Customer Database 172 and the Transaction Database 174 in its own local memory

(RAM) 154 and the transaction database 174 stores records concerning each postage indicium generated by the secure central computer 102. Therefore, one skilled in the art of computer architecture would readily realize that with this Whitehouse's system configuration, the central computers 102 cannot "process any of the plurality of security device transaction data records," because they don't have access to all users' information, some of which is stored in the local memories of the other central computers. For the same reasoning, in Whitehouse's central computers 102 environment, in which Customer Database 172 and the Transaction Database 174 are stored in each computer's own local memory (RAM) 154, a user can NOT "be authenticated using any of the cryptographic modules [allegedly, central computers]." Therefore, dependent **claims 5 and 6** are also patentable in view of Whitehouse/Pang combination for the additional limitations that they include.

In short, independent claims 1 and 39 are patentable in view of the cited references. Dependent claims 2-38 and 40-79 depend from claims 1 and 39, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested.

If the Examiner believes that a telephone conference would be useful in moving this application forward to allowance, the Examiner is encouraged to contact the undersigned at (626) 795-9900.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900